IN THE CLAIMS

Please amend the claims as follows.

Claims 1 – 27 (Cancelled)

28. (New) A multiprocessor wireless communication device comprising:

a security processor to combine first, second and third key-shares to generate a decryption key to decrypt content for the processing system, the security processor to monitor usage of the content and to purge at least one of the key-shares when the usage exceeds a measurement parameter;

a communications processor to play decrypted content received from the security processor; and

a radio-frequency (RF) interface to receive a first and second of the key-shares and encrypted content over a wireless communication link in response to a request for content and verification of a user's credit,

wherein the security processor and the communication processor are located within a processor area of an integrated circuit,

wherein communications between the security processor and the communication processor take place within the processor area to inhibit unauthorized interception of the decrypted content and interception of the third key-share stored in the processor area,

wherein the wireless communication device has the third key-share pre-stored in the processor area,

wherein the security processor authenticates the measurement parameters with an authentication code to help prevent tampering with the measurement parameters, and

wherein the measurement parameters are secured by the authentication code and provided by a security server over the wireless link along with the encrypted content or when the authentication code fails to authenticate.

29. (New) The wireless communication device of claim 28 wherein the security processor portion purges at least one of the key-shares when usage of the content exceeds a service limit indicated by the measurement parameters.

30. (New) The wireless communication device of claim 29 wherein the security processor retrieves a fourth key-share from a subscriber identity module (SIM) inserted into the wireless communication device, and receives the second key-share from a finance server when a user's credit is verified for use of the content.

31. (New) The wireless communication device of claim 30 wherein the measurement parameters comprise at least one of a date-limit, a run-time limit, and an iteration limit.

32. (New) The wireless communication device of claim 31 further comprising an applications processor located with the processor area to process applications running on the wireless communication device, and

wherein the security processor, the communications processor and the applications processor are fabricated within an application specific integrated circuit (ASIC).

33. (New) The wireless communication device of claim 32 further comprising a module receiving area to receive the subscriber identity module (SIM), the SIM having the fourth key-share pre-stored therein.